UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/672,368	09/28/2000	Francis X. McKeen	042390.P9575	7652

7590 12/09/2009

Blakely Sokoloff Taylor & Zafman LLP
12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA 90025

EXAMINER	
LANIER, BENJAMIN E	
ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
12/09/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/672,368	MCKEEN ET AL.	
	Examiner	Art Unit	
	BENJAMIN E. LANIER	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 September 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12,14,15 and 31-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12,14,15 and 31-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *9/23/2009*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 23 September 2009 has been entered.

Response to Amendment

2. Applicant's amendment filed 23 September 2009 amends claims 1-2, 9, 12, and 14-15. Claim 13 has been cancelled. Claims 31-35 have been added. Applicant's amendment has been fully considered and entered.

Response to Arguments

3. Applicant's arguments with respect to claims have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 32-35 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims are drawn to a processor readable medium described in the specification as being any medium that can be stored or transfer information (Page 11, lines 19-20). This definition is broad enough to include transmission mediums. Claims that recite nothing but the physical characteristics of a form of energy, such as a frequency, voltage, or the

strength of a magnetic field, define energy or magnetism, per se, and as such are nonstatutory natural phenomena. O'Reilly, 56 U.S. (15 How.) at 112-14. Moreover, it does not appear that a claim reciting a signal encoded with functional descriptive material falls within any of the categories of patentable subject matter set forth in §101 (MPEP 2106).

6. The Supreme Court has read the term "manufacture" in accordance with its dictionary definition to mean "the production of articles for use from raw or prepared materials by giving to these materials new forms, qualities, properties, or combinations, whether by hand-labor or by machinery." Diamond v. Chakrabarty, 447 U.S. 303, 308, 206 USPQ 193, 196-97 (1980) (quoting American Fruit Growers, Inc. v Brogdex Co., 283 U.S. 1, 11, 8 USPQ 131, 133 (1931), which in turn, quotes the Century Dictionary). Other courts have applied similar definitions. See American Disappearing Bed Co. v. Arnaelsteen, 182 F.324, 325 (9th Cir. 1910), cert. denied, 220 U.S. 622 (1911). These definitions require physical substance, which a claimed signal does not have. Congress can be presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statue without change. Lorillard v. Pons, 434 U.S. 575, 580 (1978). Thus, Congress must be presumed to have been aware of the interpretation of manufacture in American Fruit Growers when it passed the 1952 Patent Act.

7. A manufacture is also defined as the residual class of product. 1 Chisum, §1.02[3] (citing W. Robinson, The Law of Patents for Useful Inventions 270 (1890)). A product is a tangible physical article or object, some form of matter, which a signal is not. That the other two products classes, machine and composition of matter, require physical matter. A signal, a form of energy, does not fall within either of the two definitions of manufacture. Thus, a signal does not fall within one of the four statutory classes of §101.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

10. Claims 1-8, 31-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coulouris, in view of Silberschatz, in view of Summers, and further in view of Schneier, U.S Patent No. 5,978,475.

In reference to claims 1, 32:

(Coulouris et al. Section 6.3 Processes and Threads) discloses a method comprising: identifying if an event is one of a class of events to be handled in the isolated execution mode, where the isolated execution mode is a processor running a secure process (Page 168), and the event is one of an event or events that might be handled by that process, where threads within a process have their own software interrupt handling mechanisms. Handling the event using the first page table map if the event is identified as one of the class of events to be handled by the isolated execution mode, where the first page table map is the virtual memory map which maps

the memory for the running processes (page 169, 190-192), and the event identified as one of the events to be handled by the isolated execution mode is an event that is to be handled by that process. (page 172)

Coulouris et al. does not explicitly disclose maintaining a first page table map for use in an isolated execution mode and a second page table map for use in a normal execution mode. Dynamically swapping between the first page table map and the second page table map responsive to a change in execution mode.

Silberschatz et al. (p 270-271) discloses maintaining a first page table map for use in an isolated execution mode and a second page table map for use in a normal execution mode, where the first page table map is a standard process which executes its own code in an isolated manner, and the normal execution mode is the special case of shared pages between processes. Dynamically swapping between the first page table map and the second page table map responsive to a change in execution mode, where processes are isolated execution modes and changing from one execution mode to another would involve a context switch from one process that doesn't use shared pages to another that does. P. 92 (processes)

Silberschatz et al. (p 270-271) discloses that there is an advantage to sharing common code, particularly in the context of a time-sharing environment, and that reentrant shared code can result in a significant savings of total memory space. P. 271 (paragraph 2)

Neither Silberschatz et al. or Coulouris et al. explicitly recites the limitation restricting access to an isolated area of memory to bus cycles performed in the isolated execution mode by a processor operating in the isolation execution mode. However Silberschatz et al. or Coulouris et al. do disclose restricting access to an isolated area of memory. A bus, is merely the path that

connects the various components of a computer to allow data to be transferred from one internal component to another. All Buses transfer data in cycles as a synchronous device.

Summers et al. disclose Restricting access to an isolated area of memory to bus cycles performed in the isolated execution mode. (abstract) & (Column 2, lines 47-61) & (Column 3, lines 38-54), where the access to the memory via the bus are also restricted with a secure bus mechanism. Summers et al. discloses that providing an isolated path needs to be established for transmitting certain data to ensure that the data is received by authorized recipients, and that unauthorized elements have not been intercepted. (Column 1, lines 15-28) Summers et al. teaches that his invention provides an advantage over other secure bus lines by providing a secure bus arbiter module that is useable in any commercial off the shelf motherboard. (Column 1, lines 50-56) It would have been obvious to one of ordinary skill in the art at the time of invention to use the shared code processes of Silberschatz et al. with the isolated execution processes of Coulouris et al. in order to allow for significant savings in memory while still retaining the logical boundaries of the process to allow for managed concurrent execution and to use the secure bus arbiter of Summers et al. to ensure that data may be transferred securely from one module to another within the computer in a way that is compatible with off the shelf, common motherboards .

None of the previous references disclose an audit log to preserve fingerprints identifying events being processed in the isolated execution modes, the audit log to further preserver information associated with the events, the information proving current status of the isolated execution modes.

Schneier discloses creating a hash value for each entry of an event audit log (Col. 3, lines 7-19), which meets the limitation of the memory having a protected audit log to preserve fingerprints identifying events being processed in the isolated execution modes, the audit log to further preserver information associated with the events, the information proving current status of the isolated execution modes. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the audit log of Schneier into the modified teachings of Coulouris in order to provide a means to keep permanent records of critical events in a manner that is protected against attackers as taught by Schneier (Abstract & Col. 1, lines 4-10).

In reference to claims 2, 33:

(Coulouris et al. Section 6.3 Processes and Threads) discloses the method of claim 1 further comprising: Identifying if the event is one of a class of events to be handled in the isolated execution mode, where the isolated execution mode is a processor running a secure process (Page 168), and the event is one of an event or events that might be handled by that process, where threads within a process have their own software interrupt handling mechanisms. Handling the event using the first page table map if the event is identified as one of the class of events to be handled in the isolated execution mode, where the first page table map is the virtual memory map which maps the memory for the running processes(page 169, 190-192), and the event identified as one of the events to be handled by the isolated execution mode is an event that is to be handled by that process. (page 172) Wherein identifying comprises indexing into a lookup table with a exception vector of the event, where the identifying of the interrupt comprises indexing the disclosed lookup table Silberschatz et al. page (404) with the interrupt or "exception" vector page (403) & Silberschatz et al. page (402-404).

In reference to claims 3, 34:

Coulouris et al. and Silberschatz et al. discloses the method of claim 1 wherein dynamically swapping comprises: Loading a set of control registers selected based on an exception vector of the event, where a set control registers may be found with the data loaded from the interrupt descriptor table registers in the case of an event, where the control registers are the memory addresses of specialized interrupt handlers which are controlled by the event (exception) table. Silberschatz et al. page (402-404).

In reference to claims 4, 35:

Coulouris et al. and Silberschatz et al. fail to explicitly disclose the method of claim 3 wherein the set of control registers comprises: A global descriptor table register, an interrupt descriptor table register, a page table map base address register. The examiner takes as admitted prior art that a global descriptor table register and an interrupt descriptor table register were well known in the art at the time of the invention. In particular a GDTR and an IDTR are registers that contain entries which associate each interrupt or exception identifier with a descriptor for the set of instructions that are to service the event. Both of these registers are disclosed in a number of processors and processor programming manuals include the well known 80386 Programmer Reference Manual.

It would have been obvious to one of ordinary skill in the art at the time of invention to have a GDT register and an IDT register, so that processor knows which set of instructions to use to respond to a particular event.

In reference to claim 5:

Coulouris et al. and Silberschatz et al. discloses the method of claim 1 wherein maintaining

comprises: Mirroring a page table base address register. Mirroring a memory map is not explicitly disclosed however, Silberschatz et al. (page 445) discloses a RAID organization called mirroring in which the whole disk is duplicated. While costly, the advantages of this allow reading that is twice as fast. Silberschatz et al (p. 289) also discloses that memory maps, page tables, and processes may be placed on the actual hard disk itself in virtual memory. Silberschatz et al. discloses on p. 293, Figure 9.3 that page tables and memory maps for the memory may be stored in the actual hard disk. The mirroring a hard disk containing virtual memory on it as disclosed by Silberschatz et al. inherently discloses mirroring a page table base address register. Mirroring a memory map is not explicitly disclosed however, Silberschatz et al. (page 445) discloses a RAID organization called mirroring in which the whole disk is duplicated. While costly, the advantage of this allow reading that is twice as fast. Silberschatz et al (p. 289) also discloses that memory maps, page tables, and processes may be placed on the actual hard disk itself in virtual memory. Silberschatz et al. discloses on p. 293, Figure 9.3 that page tables and memory maps for the memory may be stored in the actual hard disk. The mirroring a hard disk containing virtual memory on it as disclosed by Silberschatz et al. inherently discloses, mirroring a page table base address register, and mirroring a memory map.

In reference to claim 6:

(Coulouris et al. Section 6.4 Naming and Protection) discloses the method of claim 1 further comprising defining a set of events that should be handled in isolated execution mode, where the set of events that should be handled by the isolated execution mode are the set of events that should be handled by a particular running process, selected by the server.

In reference to claim 7:

(Coulouris et al. Section 10.4 Distributed Coordination) discloses the method of claim 6 wherein the set of events to be handled in the isolated execution mode comprises: machine check events and clock events, where the machine and clock events involve the synchronization of system clocks in a distributed system.

In reference to claim 8:

Coulouris et al. discloses the method of claim 2 wherein handling comprises determining if a current mode is the isolated execution mode, where the current mode is determined if it is in isolated execution mode, if it is determined that an isolated process is currently running. (Section 6.4 Naming and Protection). Loading a set of control registers with values corresponding to the first page table map if the current mode is not the isolated execution mode and the event is one of the class, where the set of control registers are loaded which contain the descriptor for the set of instructions needed to handle the current event, if it is found that the event is not to be handled by the current running process, but by another process. (Section 6.4 Naming and Protection). Dispatching an exception vector after the loading is complete, where the exception vector for the event is be dispatched once the new process capable of handling the event is loaded or switched to. (Section 6.4 Naming and Protection) & Figure 6.12.

In reference to claim 31:

Summers discloses physical isolation of a single computer bus to a single data class for a given data transfer thereby insulating it from devices associated with any other data class (Col. 5, lines 7-13), which meets the limitation of the processor operating in the isolation execution mode via an isolated execution circuitry at the processor, and wherein restricting access includes protecting the isolated area by access checks, and permitting access to the isolated area via

special bus cycles issued by a processor. It would have been obvious to one of ordinary skill in the art at the time of invention to use the shared code processes of Silberschatz et al. with the isolated execution processes of Coulouris et al. in order to allow for significant savings in memory while still retaining the logical boundaries of the process to allow for managed concurrent execution and to use the secure bus arbiter of Summers et al. to ensure that data may be transferred securely from one module to another within the computer in a way that is compatible with off the shelf, common motherboards.

11. Claims 9-12, 14-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Takahashi, U.S. Patent No. 5,615,263, in view of Silberschatz , in view of Summers, U.S. Patent No. 6,098,133, and further in view of Schneier, U.S Patent No. 5,978,475.

In reference to claim 9:

Takahashi discloses an apparatus comprising: A first storage location storing control data for a first page table map for use in an isolation execution mode, where the first page table map is the map that designates the memory. (Figure 5) & (Column 3, lines 45-60) & (Column 4, lines 23-60) & (Column 3, lines 25-40). A second storage location storing control data for a second page table map for use in a normal execution mode, where the second storage location is the ROM. (Figure 5) & (Column 3, lines 45-60) & (Column 4, lines 23-60) & (Column 3, lines 25-40). A selection unit to select which page table map is applied responsive to receipt of an event, where the selection unit chooses to select between the ROM and the memory based on the execution mode of the processor. (Figure 5) & (Column 3, lines 45-60) & (Column 4, lines 23-60) & (Column 3, lines 25-40) & (Column 2, lines 45 - 61).

Takahashi fails to disclose dynamically swapping between the first page table map and the second page table map responsive to a change in execution mode. Silberschatz discloses dynamically swapping between the first page table map and the second page table map responsive to a change in execution mode, where processes are isolated execution modes and changing from one execution mode to another would involve a context switch from one process that doesn't use shared pages to another that does. P. 92 (processes). It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the page swapping of Silberschatz into the protected system of Takahashi in order to allow for significant savings in memory while still retaining the logical boundaries of the process to allow for managed concurrent execution.

Takahashi fails to explicitly disclose an isolated execution circuit to generate isolated access bus cycles. Wherein isolated access bus cycles are to be used if the apparatus operates in an isolated execution mode.

Summers et. al. discloses an isolated execution circuit to generate isolated access bus cycles, (abstract) & (Column 2, lines 47-61) & (Column 3, lines 38-54), where the access to the memory via the bus are also restricted with a secure bus mechanism. Wherein isolated access bus cycles are to be used if the apparatus operates in an isolated execution mode (abstract) & (Column 2, lines 47-61) & (Column 3, lines 38-54) & (Column 2, line 60 - Column 3, line 15), where the access to the memory via the bus are also restricted with a secure bus mechanism. Summers et al. discloses that providing an isolated path needs to be established for transmitting certain data to ensure that the data is received by authorized recipients, and that unauthorized elements have not been intercepted. (Column 1, lines 15-28) Summers et al. teaches that his

invention provides an advantage over other secure bus lines by providing a secure bus arbiter module that is useable in any commercial off the shelf motherboard. (Column 1, lines 50-56). It would have been obvious to one of ordinary skill in the art at the time of invention to use the secure bus arbiter of Summers et al. to ensure that data may be transferred securely from one module to another within the computer in a way that is compatible with off the shelf, common motherboards.

None of the previous references disclose an audit log to preserve fingerprints identifying events being processed in the isolated execution modes, the audit log to further preserver information associated with the events, the information proving current status of the isolated execution modes.

Schneier discloses creating a hash value for each entry of an event audit log (Col. 3, lines 7-19), which meets the limitation of the memory having a protected audit log to preserve fingerprints identifying events being processed in the isolated execution modes, the audit log to further preserver information associated with the events, the information proving current status of the isolated execution modes. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the audit log of Schneier into the modified teachings of Takahashi in order to provide a means to keep permanent records of critical events in a manner that is protected against attackers as taught by Schneier (Abstract & Col. 1, lines 4-10).

In reference to claim 10:

Takahashi and Summers et al. discloses the apparatus of claim 9 wherein the selection unit comprises a multiplexer that selects between the first and second storage locations based on an exception vector of the event. (Figure 1, Item 13) & (Column 2, line 62 - Column 3, line 15)

In reference to claim 11:

Takahashi and Summers et al. (Figure 5) & (Column 3, lines 45-60) & (Column 4, lines 23-60) & (Column 3,lines 25-40) & (Column 2, lines 45 - 61) discloses the apparatus of claim 9 wherein the first storage location contains a base address for the first page table map and the second storage location contains a base address for the second page table map.

In reference to claim 12:

Takahashi discloses a platform comprising a processor executing in one of a normal execution mode and an isolated execution mode associated with an isolated area of memory (Column 2, lines 45 - 61). A first set of control registers to define a current memory map of the platform (Column 3, lines 45-60). A mapping unit to dynamically load the first set of control registers responsive to an event if the event should be handled using an alternative memory map (Figure 5) & (Column 3, lines 45-60) & (Column 4, lines 23-60) & (Column 3,lines 25-40).

Takahashi does not disclose a first/second set of registers having a first/second subset corresponding to control register values for a normal execution mode memory map and an isolated execution mode memory map, dynamically swapping between the first/second subsets. Silberschatz a first/second set of registers having a first/second subset corresponding to control register values for a normal execution mode memory map and an isolated execution mode memory map, dynamically swapping between the first/second subsets (pages 92 & 270-271). It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the page swapping of Silberschatz into the protected system of Takahashi in order to allow for significant savings in memory while still retaining the logical boundaries of the process to allow for managed concurrent execution.

None of the previous references disclose an audit log to preserve fingerprints identifying events being processed in the isolated execution modes, the audit log to further preserver information associated with the events, the information proving current status of the isolated execution modes.

Schneier discloses creating a hash value for each entry of an event audit log (Col. 3, lines 7-19), which meets the limitation of the memory having a protected audit log to preserve fingerprints identifying events being processed in the isolated execution modes, the audit log to further preserver information associated with the events, the information proving current status of the isolated execution modes. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the audit log of Schneier into the modified teachings of Takahashi in order to provide a means to keep permanent records of critical events in a manner that is protected against attackers as taught by Schneier (Abstract & Col. 1, lines 4-10). Takahashi fails to explicitly disclose an isolated execution circuit to generate isolated access bus cycles if the processor is executing in the isolated execution mode.

Summers et al. discloses an isolated execution circuit to generate isolated access bus cycles if the processor is executing in the isolated execution mode (abstract) & (Column 2, lines 47-61) & (Column 3, lines 38-54), which meets the limitation of permit the processor to access the isolated area to operate in the isolated execution mode. Summers et al. discloses that providing an isolated path needs to be established for transmitting certain data to ensure that the data is received by authorized recipients, and that unauthorized elements have not been intercepted (Column 1, lines 15-28), which meets the limitation of restrict access to the isolated area. Summers et al. teaches that his invention provides an advantage over other secure bus lines by

providing a secure bus arbiter module that is useable in any commercial off the shelf motherboard. (Column 1, lines 50-56). It would have been obvious to one of ordinary skill in the art at the time of invention to use the secure bus arbiter of Summers et al. to ensure that data may be transferred securely from one module to another within the computer in a way that is compatible with off the shelf, common motherboards.

In reference to claim 14:

Takahashi and Summers et al. discloses the platform of claim 13 wherein the selection unit comprises a multiplexer having selection driven by an exception vector of an incoming event. (Figure 1, Item 13) & (Column 2, line 62 - Column 3, line 15). However the use of multiple multiplexers is not explicitly disclosed. The Examiner takes official notice that using a plurality of multiplexers as opposed to a single multiplexer was well known in the art at the time of invention.

In fact, multiple multiplexers may be used without any change to the input and output of a digital system as opposed to a single multiplexer if arranged to be logically equivalent. It would have been obvious to one of ordinary skill in the art at the time of invention to use multiple multiplexers to combine different size data streams into a single larger data stream.

In reference to claim 15:

Takahashi and Summers et al. fails to explicitly disclose the platform of claim 12 wherein the first set of control registers comprises a global descriptor table register; an interrupt description table register; a page table map base address register. The examiner takes as admitted prior art that a global descriptor table register and an interrupt descriptor table register were well known in the art at the time of the invention as part of a processor. In particular a GDTR and an

IDTR are registers that contain entries which associate each interrupt or exception identifier with a descriptor for the set of instructions that are to service the event. Both of these registers are disclosed in a number of processors and processor programming manuals include the well known 80386 Programmer Reference Manual. It would have been obvious to one of ordinary skill in the art at the time of invention to have a GDT register and an IDT register, so that processor knows which set of instructions to use to respond to a particular event.

12. Claims 9-12, 14-15 rejected under 35 U.S.C. 103(a) as being unpatentable over Poisner, U.S. Patent No. 5,729,760, in view of Silberschatz , in view of Summers, U.S. Patent No. 6,098,133, and further in view of Schneier, U.S Patent No. 5,978,475.

In reference to claim 9:

Poisner discloses an apparatus comprising A first storage location storing control data for a first page table map for use in an isolation execution mode, where the first table map is the unrestricted memory as indicated by the IO mapped register. (Figure 8) & (Column 2, lines 55 - Column 3, lines 52) & (Column 4, lines 42-67) A second storage location storing control data for a second page table map for use in a normal execution mode, where the second table map is the restricted memory as indicated by the IO mapped register. (Figure 8) & (Column 2, lines 55 - Column 3, lines 52) & (Column 4, lines 42-67) A selection unit to select which page table map is applied responsive to receipt of an event, where the selection unit makes the determination based on the mode of processor execution. (Figure 8) & (Column 2, lines 55 - Column 3, lines 52) & (Column 4, lines 42-67)

Poisner fails to explicitly disclose an isolated execution circuit to generate isolated access bus cycles wherein isolated access bus cycles are to be used if the apparatus operates in an isolated execution mode.

Summers et. al. discloses an isolated execution circuit to generate isolated access bus cycles, (abstract) & (Column 2, lines 47-61) & (Column 3, lines 38-54), where the access to the memory via the bus are also restricted with a secure bus mechanism wherein isolated access bus cycles are to be used if the apparatus operates in an isolated execution mode (abstract) & (Column 2, lines 47-61) & (Column 3, lines 38-54) & (Column 2, line 60 - Column 3, line 15), where the access to the memory via the bus are also restricted with a secure bus mechanism. Summers et al. discloses that providing an isolated path needs to be established for transmitting certain data to ensure that the data is received by authorized recipients, and that unauthorized elements have not been intercepted. (Column 1, lines 15-28) Summers et al. teaches that his invention provides an advantage over other secure bus lines by providing a secure bus arbiter module that is useable in any commercial off the shelf motherboard. (Column 1, lines 50-56) It would have been obvious to one of ordinary skill in the art at the time of invention to use the secure bus arbiter of Summers et al. to ensure that data may be transferred securely from one module to another within the computer in a way that is compatible with off the shelf, common motherboards.

Takahashi fails to disclose dynamically swapping between the first page table map and the second page table map responsive to a change in execution mode. Silberschatz discloses dynamically swapping between the first page table map and the second page table map responsive to a change in execution mode, where processes are isolated execution modes and

changing from one execution mode to another would involve a context switch from one process that doesn't use shared pages to another that does. P. 92 (processes). It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the page swapping of Silberschatz into the protected system of Takahashi in order to allow for significant savings in memory while still retaining the logical boundaries of the process to allow for managed concurrent execution.

None of the previous references disclose an audit log to preserve fingerprints identifying events being processed in the isolated execution modes, the audit log to further preserver information associated with the events, the information proving current status of the isolated execution modes.

Schneier discloses creating a hash value for each entry of an event audit log (Col. 3, lines 7-19), which meets the limitation of the memory having a protected audit log to preserve fingerprints identifying events being processed in the isolated execution modes, the audit log to further preserver information associated with the events, the information proving current status of the isolated execution modes. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the audit log of Schneier into the modified teachings of Takahashi in order to provide a means to keep permanent records of critical events in a manner that is protected against attackers as taught by Schneier (Abstract & Col. 1, lines 4-10).
In reference to claim 10:

Poisner (Column 8, line 42 - Column 9, line 15) discloses the apparatus of claim 9 wherein the selection unit comprises a multiplexer that selects between the first and second

storage locations based on an exception vector of the event.

In reference to claim 11:

Poisner (Figure 8) & (Column 2, lines 55 - Column 3, lines 52) & (Column 4, lines 42-67) discloses the apparatus of claim 9 wherein the first storage location contains a base address for the first page table map and the second storage location contains a base address for the second page table map.

In reference to claim 12:

Poisner discloses a platform comprising a processor executing in one of a normal execution mode and isolated execution mode associated with an isolated area of memory, where the normal mode of execution is the mode of execution that uses the unrestricted IO map and the isolated mode of execution uses the restricted IO map. (Figure 8) &(Column 2, lines 55 - Column 3, lines 52) & (Column 4, lines 42-67) A first set of control registers to define a current memory map of the platform, where the IO memory maps are defined in the control registers. (Figure 8) & (Column 2, lines 55 - Column 3, lines 52) & (Column 4, lines 42-67) A mapping unit to dynamically load the first set of control registers responsive to an event if the event should be handled using an alternative memory map, where the memory map are the different memories accessed depending on the different modes of execution for the processor, and each memory map is dynamically loaded based on the mode of the processor. (Figure 8) & (Figure 9) & (Figure 10) & (Column 2, lines 55 - Column 3, lines 52) & (Column 4, lines 42-67)

Takahashi does not disclose a first/second set of registers having a first/second subset corresponding to control register values for a normal execution mode memory map and an isolated execution mode memory map, dynamically swapping between the first/second subsets.

Silberschatz a first/second set of registers having a first/second subset corresponding to control register values for a normal execution mode memory map and an isolated execution mode memory map, dynamically swapping between the first/second subsets (pages 92 & 270-271). It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the page swapping of Silberschatz into the protected system of Takahashi in order to allow for significant savings in memory while still retaining the logical boundaries of the process to allow for managed concurrent execution.

None of the previous references disclose an audit log to preserve fingerprints identifying events being processed in the isolated execution modes, the audit log to further preserver information associated with the events, the information proving current status of the isolated execution modes.

Schneier discloses creating a hash value for each entry of an event audit log (Col. 3, lines 7-19), which meets the limitation of the memory having a protected audit log to preserve fingerprints identifying events being processed in the isolated execution modes, the audit log to further preserver information associated with the events, the information proving current status of the isolated execution modes. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the audit log of Schneier into the modified teachings of Takahashi in order to provide a means to keep permanent records of critical events in a manner that is protected against attackers as taught by Schneier (Abstract & Col. 1, lines 4-10).

Poisner does not explicitly disclose An isolated execution circuit to generate isolated access bus cycles if the processor is executing in the isolated execution mode.

Summers et al. discloses an isolated execution circuit to generate isolated access bus cycles if the processor is executing in the isolated execution mode. (abstract) & (Column 2, lines 47-61) & (Column 3, lines 38-54) Summers et al. discloses that providing an isolated path needs to be established for transmitting certain data to ensure that the data is received by authorized recipients, and that unauthorized elements have not been intercepted. (Column 1, lines 15-28) Summers et al. teaches that his invention provides an advantage over other secure bus lines by providing a secure bus arbiter module that is useable in any commercial off the shelf motherboard. (Column 1, lines 50-56) It would have been obvious to one of ordinary skill in the art at the time of invention to use the secure bus arbiter of Summers et al. to ensure that data may be transferred securely from one module to another within the computer in a way that is compatible with off the shelf, common motherboards.

In reference to claim 14:

Poisner (Column 8, line 42 - Column 9, line 15) discloses the platform of claim 13 wherein the selection unit comprises a multiplexer having selection driven by an exception vector of an incoming event. However the use of multiple multiplexers is not explicitly disclosed. The Examiner takes official notice that using a plurality of multiplexers as opposed to a single multiplexer was well known in the art at the time of invention. Multiple multiplexers may be used without any change to the input and output of a digital system as opposed to a single multiplexer if arranged to be logically equivalent. It would have been obvious to one of ordinary skill in the art at the time of invention to use multiple multiplexers to combine different size data streams into a single larger data stream.

In reference to claim 15:

Poisner fails to explicitly disclose the platform of claim 12 wherein the first set of control registers comprising a global descriptor table register, an interrupt description table register, a page table map base address register. The examiner takes as admitted prior art that a global descriptor table register and an interrupt descriptor table register were well known in the art at the time of the invention as part of a processor. In particular a GDTR and an IDTR are registers that contain entries which associate each interrupt or exception identifier with a descriptor for the set of instructions that are to service the event. Both of these registers are disclosed in a number of processors and processor programming manuals include the well known 80386 Programmer Reference Manual. It would have been obvious to one of ordinary skill in the art at the time of invention to have a GDT register and an IDT register, so that processor knows which set of instructions to use to respond to a particular event.

Conclusion

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN E. LANIER whose telephone number is (571)272-3805. The examiner can normally be reached on M-Th 7:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432